Digital Evidence:
How to Collect and send it to Digital Forensic Lab

Presented by:

ELIAS HOSSEN
Police Inspector
Special Action Group
Counter Terrorism & Transnational Crime
Dhaka Metropolitan Police
saymeonline@gmail.com
+8801919933221

Education:

B.Ed (Hon's), M.Ed, PGDICT, M.Sc (Cyber Security)

Training Course completed:

- Enhancement of Cyber Crime Investigation Capability of Bangladesh Police, Soonchunhyang University (SCH), South Korea, June 2014.
- Cyber Security Course, Gujarat Forensic Science University, India, October 2016.
- Exploit Hackers Tools & Technique, Singapore, October 2018.
- Boot Camp on Access Data FTK Forensic, UAE Dubai, December, 2018.
- Windows Forensic, Singapore, March 2019.

Job Experience:

- Working as a Digital forensic Expert & Cyber Crime Investigator at Digital Forensics Forensic Lab, CID from February 2012 to July 2021.

Experience as a Facilitator:

- From 2013 to till today I have conducted training in different institute like Bangladesh Police Academy(Sardah, Rajshahi), Forensic Training Institute (CID), Detective Training School (CID), Cyber Crime Investigation Training Center, Police Training Center (PTC) and Air Force Intelligence School (Kurmitola, Dhaka).

UN Mission Experience:

- Served as Police Advisor in the United Nations Mission in South Sudan from February 2017 to February 2018.

What is Digital Evidence?

Information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination.

Digital Security Act 2018

Digital Security Act 2018 Under section 2(i) "Digital" means the working procedure based on binary system (0 or 1) or digit based system, and to fulfill the objective of this Act, electrical, digital, magnetic, optical, biometric, electrochemical, electromechanical, wireless or electro-magnetic technology will be the part of it;

ডিজিটাল নিরাপত্তা আইন ২০১৮ এর ২(ঝ) "ডিজিটাল" অর্থ যুগ্ম-সংখ্যা (০ ও ১/বাইনারি) বা ডিজিট ভিত্তিক কার্য পদ্ধতি, এবং এই আইনের উদ্দেশ্য পূরণকল্পে, ইলেকট্রিক্যাল, ডিজিটাল ম্যাগনেটিক, অপটিক্যাল, বায়োমেট্রিক, ইলেকট্রোকেমিক্যাল, ইলেকট্রোমেকানিক্যাল, ওয়্যারলেস বা ইলেকট্রোম্যাগনেটিক টেকনোলজিও ইহার অন্তর্ভুক্ত হইবে;

Digital evidence -

Is latent, like fingerprints or DNA evidence.

- digital evidence may also contain physical evidence such as DNA, fingerprints, or serology. Physical evidence should be preserved for appropriate examination.

5 Key Facts About Digital Evidence

1. Many types of crime involve digital evidence.
2. Every crime scene is a digital evidence crime scene.
3. Digital evidence can be fragile.
4. Digital evidence can be easily altered.
5. Never assume that digital evidence is destroyed

SPECIAL PROBLEMS IN DIGITAL EVIDENCE

1. Digital evidence is extremely time sensitive – especially in the case of Logs and Telecommunications data
2. Crosses jurisdictional borders quickly and easily
3. Chain of custody needs to be maintained
4. All evidence needs to be authenticated

Criminal Uses Of Digital Evidence

1. Target of a crime
2. Instrument of a crime
3. Repository of evidence that documents the crime itself.
   ➔ Universal
   ➔ Case specific

Sources Of Digital Evidence

Three basic sources:

- User's Activities/Artifacts
- System Information (including backups/archive)
- Network/communications logs

Tools and Materials for Collecting Digital Evidence

1. Cameras (photo and video)
2. Cardboard boxes
3. Notepads
4. Gloves
5. Evidence inventory logs
6. Evidence tape
7. Paper evidence bags
8. Evidence stickers, labels, or tags
9. Crime scene tape
10. Anti-static bags
11. Permanent markers
12. Nonmagnetic tools
13. Radio frequency-shielding material (faraday isolation bags or aluminum foil)

Forensic Tools (Hardware & Software)

1. Write Blockers to preview suspected storage media in read only mode
2. Disk Duplicators
3. Portable Workstation
4. Instant Passwords Recovery/Breaking Software
5. Disk Forensic Software/Triage
6. Device for Seizing Communication Devices like Cell phone, SIM, GPS, Sat Phone etc.

Handle of Digital Evidence at Crime Scene

Step- 01
Securing and Evaluating the Scene

- **Primary consideration should be……**
- Safety
- Protect the evidence from harm
- visually identify all potential evidence
- ensure that the integrity of both the digital and traditional evidence is preserved
- Secure Crime Scene with Tapes
- Immediately secure all electronic devices, including personal or portable devices
- Take photographs of place from different angles
- Note all details
- Document the entire scene and the specific location of the evidence found

- Ensure that no unauthorized person has access to any electronic devices at the crime scene
- If someone is working on PC when you reached then ask & insist him/her to leave the terminal
- Refuse offers of help or technical assistance from any unauthorized persons
- Remove all persons from the crime scene or the immediate area from which evidence is to be collected;
- Remove all persons from the crime scene or the immediate area from which evidence is to be collected;
- Ensure that the condition of any electronic device is not altered;
- Leave a computer or electronic device off if it is already turned off;
- If required then ask expert to develop latent prints and collect trace or biological evidence on keyboard, mouse, tables etc;

When the computer is on or the power state cannot be determined, then……

- Look and listen for indications;
- Listen for the sound of fans running, drives spinning;
- Check to see if light emitting diodes (LEDs) are on;

Check the display screen for signs that digital evidence is being destroyed……

<u>Words to look out for:</u>

- Delete
- Format
- Remove
- Copy
- Move
- cut
- wipe

✓ Look for indications that the computer is being accessed from a remote computer or device;

- ✓ Look for signs of active or ongoing communications with other computers or users such as instant messaging windows or chat rooms;
- ✓ Take note of all cameras or Web cameras (Web cams) and determine if they are active;

Step 02

Identifying Digital Evidence

Digital Evidence typically falls into four distinct categories:

1. Commonplace

- ✓ Traditional digital media that often hides in plain view

2. Obscure

- ✓ Non-traditional digital media

3.Protected

- ✓ Bio-metric protected
- ✓ Mechanically protected
- ✓ Concealed
- ✓ Digital evidence can be found any where and in any form so keep your eyes opened;

It can be

It can also be found in many ways….:

Step- 03
Preliminary Interviews

- all users of the computers and devices;
- computer and Internet user information;
- login names and user account names;

- purpose and uses of computers and devices;
- passwords;
- automated applications in use;
- type of Internet access;

- offsite storage;
- internet service provider;
- installed software documentation;
- e-mail accounts;
- security provisions in use;
- web mail account information;
- data access restrictions in place;
- instant message screen names;
- destructive devices or software in use;

- online social networking;
- web site account information;
- other relevant information;

Step- 04
Documentation the Scene

Take Notes

- Who
- Times
- Description of the device

- **Sketch the Scene**
- Take Photographs
- Active Screen
- Passwords
- Books
- Back of the Computers (Casing)

Step- 05
Evidence Collection & Preservation

Precautions:

- **Legal authority exits to Seize Evidence;**
- Improper powered off during digital evidence collection –

encrypted data may become inaccessible

- without proper training and skills should not –
- attempt to explore the contents of

Or

- to recover information from a computer or other electronic device

Once identified then lets acquire but wait

- In what state the evidence is

  -Live (Turned on PC/Laptop/ Cell-phone)

  -Or Dead(OFF PC/Laptop/ Cell-phone)

Method of data extraction is state dependent

Collection of Digital Device when it is Live/On

- ✓ Live Acquisition/Triage Operation
- ✓ Shutdown the System

- Hard Shutdown
- Graceful Shutdown

When we pull the power we loose

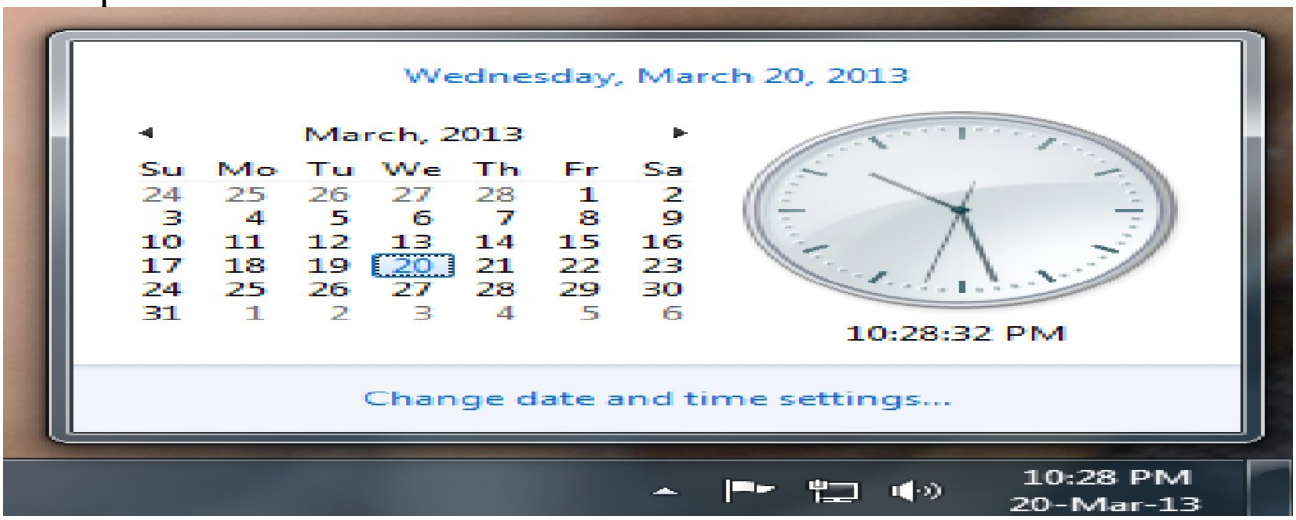
-All Volatile information

To preserve volatile data …..

- Live Acquisition/Triage Operation

<u>For Live Acquisition, we can do…..:</u>

- Take photo of screen with date and time window with time zone.



Use a CD or trusted PENDRIVE to execute the triage tools

- capture the RAM, Registry and other user defined items from user defined location .

- allow to perform keyword searching on running PC to check whether it is having information of your interest.

But when the experienced personnel assistance or triage tools is not available, then……

When the PC is ON-

- Do not use computer or attempt to search for evidence.

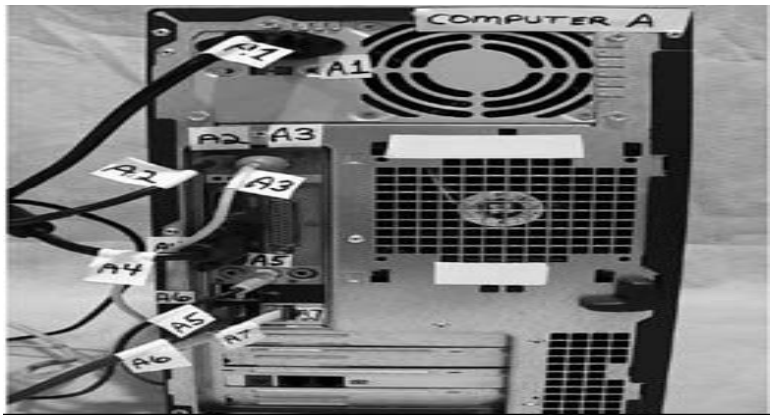
- Take photo of screen with date and time window with time zone.
- Photograph computer front and back as well as cords and connected devices, as found.

- Photograph surrounding area prior to moving any evidence.

- If computer is “on” and something is displayed on the monitor, photograph the screen.

Unplug power cord from back of tower.

Diagram and label cords to later identify connected devices.



- **<u>Photograph the distinctively labeled cords, cables,</u>** wires, and USB drives and the corresponding labeled connections;
- Place tape over the floppy disk slot, if present;
- Tape the CD/DVD drive slot closed to prevent it from opening;
- Place tape over the power switch;
- Record the make, model, serial numbers, and any user-applied markings or identifiers;

When the PC is OFF-

- **If computer is “off”, do not turn “on”**
- Document, photograph, and sketch all wires, cables, and other devices;

- Distinctively label the power supply cord and all cables, wires, or USB drives attached as well as corresponding connections;
- Photograph the distinctively labeled cords, cables, wires, and USB drives and the corresponding labeled connections;
- Remove and secure the power supply cord from the back and from the wall outlet;
- Disconnect and secure all cables, wires, and USB drives from the computer and document the device or equipment connected at the opposite end;
- Place tape over the floppy disk slot, if present;
- Tape the CD/DVD drive slot closed to prevent it from opening;
- Place tape over the power switch;
- Record the make, model, serial numbers, and any user-applied markings or identifiers;

For laptop computers:

- Document, photograph, and sketch all wires, cables, and devices connected to the laptop computer.
- Uniquely label all wires, cables, and devices connected to the laptop computer as well as the connection they occupied.
- Photograph the uniquely labeled cords, cables, wires, and devices connected to the laptop computer and the corresponding labeled connections they occupied.
- Remove and secure the power supply and all batteries from the laptop computer.
- Disconnect and secure all cables, wires, and USB drives from the computer and document the equipment or device connected at the opposite end.

- Place tape over the floppy disk slot, if present.
- Make sure that the CD or DVD drive trays are retracted into place; note whether these drive trays are empty, contain disks, or are unchecked; and tape the drive slot closed to prevent it from opening.
- Place tape over the power switch.
- Record the make, model, serial numbers, and any user-applied markings or identifiers.

Network Server/Business Network:

- Consult a computer specialist for further assistance
- Secure the scene and do not let anyone touch except personnel trained to handle network systems.
- Pulling the plug could:
    - Severely damage the system
    - Disrupt legitimate business
    - Create officer and department liability

5 Key Facts About Handling Mobile Phones

1. Access the Situation

- ➢ Leave the phone on
- ◆ Handle a password protected/Encrypted device
- ◆ Monitor Incoming Information
- ◆ Block Signals

- **Leave the phone off**
  - Preserve Evidence
  - Safeguard the Evidence

2. Don't Browse

3. Look for Peripherals & SIM Cards

4. Find Passwords

5. Don't assume that the device was destroyed

➔ **Seize peripherals such as the battery charger/cables and SIM card if possible.**

Handling PDAs

- Seize the Cradle

- If you turn it off, plug into a battery charger when you return to your office
- Data Loss is a concern because PDAs may lose data once power is lost.

Handling USB Devices

Dos…..

- Seal in an evidence bag until examined
- Document what you review and the precautions taken to preserve the digital evidence
- Use write protection if available

Don't place these device near…..

- Heat
- Cold

- Magnets or RF emitter

Handling Memory Cards

Dos…..

- Seal in an evidence bag until examined
- Document what you review and the precautions taken to preserve the digital evidence
- Use write protection if available
- Leave the memory card in a digital camera if it is in the same compartment as the battery

Don't place these device near…..

- Heat
- Cold
- Magnets or RF emitter

Handling Digital Cameras

Dos…..

- Turn the camera off and Seal in an evidence bag later examined
- Document what you review and the precautions taken to preserve the digital evidence
- Seize the entire device and all accessories
- Submit cameras with volatile internal memory to an examiner asp

Don't…..

- Browse
- Remove the battery

- Remove the memory card in a digital camera if it is in the same compartment as the battery
- Turn the camera on if already off
- Place these device near….. Heat/Cold/Magnets or RF emitter

বিশেষ সতর্কতা

১। যেকোন আলামত বিশেষ করে যে সকল আলামত **Live/On** অবস্থায় পাওয়া যাবে তা জব্দ করার সময় অবশ্যই তারিখ এবং সময় দেখে নোট নিতে হবে। অনেকে **Intentionally system date & time** পরিবর্তন করে রাখে।

২। জব্দ করার পরে কোন আলামত চালু করা যাবে না বা দেখার জন্য ব্রাউজ করা যাবে না, যদি দেখতেই হয় তবে **Forensic software** ব্যবহার করে দেখতে হবে। আইটি বিশেষজ্ঞ **Forensic software** দ্বারা পরীক্ষা করার সময়ে বিশেষ করে কম্পিউটার বা ল্যাপটপে ব্যবহৃত স্টোরেজ ডিভাইসের **Last Access Date** জব্দ করার পরে দেখালে আলামতের **Chain of Custody** প্রশ্নবিদ্ধ হবে।

Packaging, Transportation, and Storage of Digital Evidence

➔ **Digital evidences are fragile and sensitive**

1. to extreme temperatures
2. humidity,
3. physical shock
4. static electricity
5. magnetic fields;

➔ **Take precautions to avoid altering, damaging, or destroying the data -**

1. documenting
2. Photographing
3. packaging
4. transporting
5. storing

➔ **Pack in antistatic packaging like-**

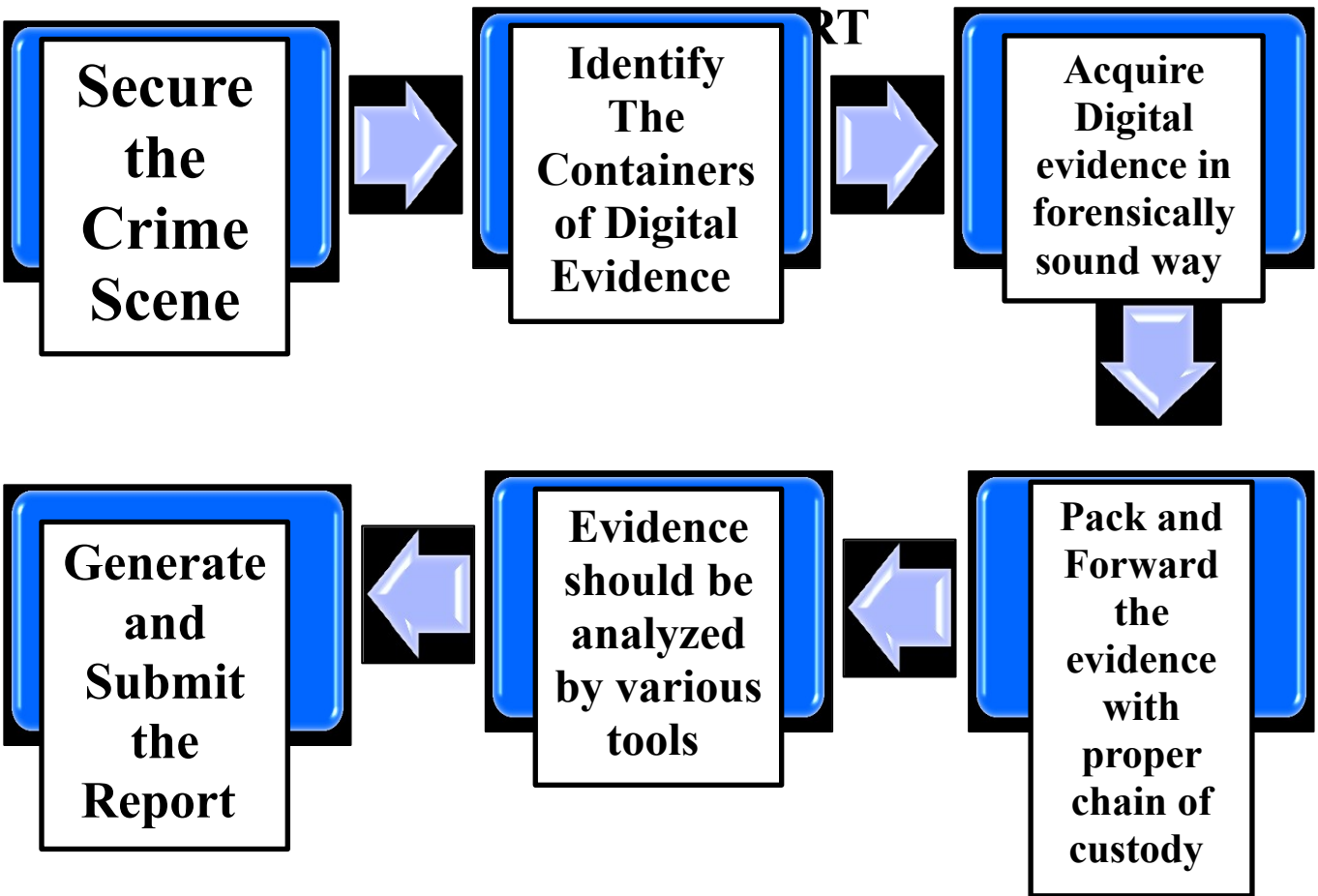
1. paper bags
2. envelopes
3. cardboard boxes

4. antistatic storage containers

➔ **Packaged in a manner that will prevent from –**
1. being bent
2. scratched
3. otherwise deformed;

➔ Avoid packing whole PC Cabinet. Instead just seize Hard Drive/s and other material
➔ avoid keeping digital evidence in a vehicle for prolonged periods of time;
➔ ensure that the digital evidence is stored in a secure, climate-controlled environment;
➔ ensure that the digital evidence is not exposed to
a. magnetic fields
b. Moisture
c. Dust
d. Vibration
e. any other elements that may damage or destroy it

➔ ensure to maintain chain of custody;


Secure the Crime Scene
Identify The Containers of Digital Evidence
Acquire Digital evidence in forensically sound way
Pack and Forward the evidence with proper chain of custody
Evidence should be analyzed by various tools
Generate and Submit the Report

আলামত সংগ্রহকালিন প্রতিবন্ধকতা সমূহঃ

১। ইউনিট ভিত্তিক প্রশিক্ষিত জনবলের অভাব রয়েছে। সিআইডি সাইবার ইনভেস্টিগেশন ইউনিট, ঢাকা; ডিএমপি সাইবার ইনভেস্টিগেশন ইউনিট, পিবিআই সাইবার ইনভেস্টিগেশন ইউনিট, ঢাকায় মামলা রুজুর ব্যবস্থা নাই, মামলা দায়ের করতে হলে একজন ভিক্টিমকে থানায় যেতে হয়, অধিকাংশ থানাতে বিষয় সংশ্লিষ্ট প্রশিক্ষিত একাধিক জনবল সব সময় পাওয়া যায় না। যে কারনে মামলা পরবর্তী সময়ে আলামত জব্দ করা সঠিকভাবে হয়না।

২। মাঠ পর্যায়ে থানা ভিত্তিক ক্রাইম সিন ইউনিট না থাকায় আলামত সংগ্রহের কাজে "ক্রাইম সিন ইউনিটের" সহযোগীতা সার্বক্ষনিক পাওয়া যায় না। মাঠ পর্যায়ের অফিসারদের পর্যায়ক্রমে ডিজিটাল ইভিডেন্স কালেকশন ও ব্যবস্থাপনার করার বিষয়ে একই অফিসারকে একাধিক প্রশিক্ষন প্রদানের ব্যবস্থা নাই।

৩। মাঠ পর্যায়ের ইউনিট সমূহে ডিজিটাল আলামত সংগ্রহ করার জন্য ফরেনসিক টুল কিটস নাই, থাকলেও পর্যাপ্ত নয় এবং প্রশিক্ষিত জনবল নেই।

৪। আলামত প্যাকেজিং ও পরিবহনের ক্ষেত্রে বিশেষ কোন সতর্কতা অবলম্বন করা হয়না, গতানুগতিকভাবে প্যাকেজিং ও পরিবহন করা হয়।

আলামত ফরেনসিক ল্যাবে যেভাবে পাঠাতে হয়

১। মামলার আলামত পরীক্ষার জন্য বিজ্ঞ আদালত কর্তৃক আদেশনামা ও ক্ষমতাপত্র সংগ্রহ করতে হবে (যে সংস্থার মাধ্যমে পরীক্ষা করাতে চান, সেই সংস্থার নাম আদেশনামা ও ক্ষমতাপত্রে উল্লেখ করতে হবে) এবং পরীক্ষার জন্য সংশ্লিষ্ট সংস্থা বরাবরে আবেদন করতে হবে।

২। মামলা প্রমানের জন্য সম্ভাব্য কি ধরনের তথ্যাদি প্রয়োজন তা আবেদনে চাহিত বিষয়ে সুস্পষ্টভাবে উল্লেখ করতে হবে।

৩। সংযুক্ত হিসেবে (ক) জব্দ তালিকা এবং (খ) মামলার এজাহার প্রদান করতে হবে।

৪। তদন্তকালে প্রাপ্ত বিভিন্ন ধরনের তথ্যাদি মুখবন্দ খামে প্রদান করা যেতে পারে।

আলামত পরীক্ষার জন্য পাঠানো যেতে পারে

১। ডিজিটাল ফরেনসিক ল্যাব, সিআইডি, ঢাকা।

২। পিবিআই ফরেনসিক ল্যাব, পিবিআই হেডঃ, ঢাকা।

৩। ডিজিটাল ফরেনসিক ল্যাব, **BGD e-GOV CIRT,** বাংলাদেশ কম্পিউটার কাউন্সিল, ই-১৪/এক্স

আইসিটি টাওয়ার, আগারগাও ঢাকা-১২০৭, বাংলাদেশ।

ফরেনসিক ল্যাবে যেভাবে মামলার আলামত রাখা হয়

১। ফরেনসিক পরীক্ষার জন্য প্রেরীত আবেদন, বিজ্ঞ আদালত কর্তৃক সংগৃহীত আদেশনামা এবং ক্ষমতাপত্রে উল্লেখিত আলামতের বর্ণনা জব্দতালিকায় উল্লেখিত বর্ণনার সাথে হুবহু মিলে কিনা তা যাচাই করা হয়।

২। প্রদত্ত আলামত গুলো সচল বা ত্রুটিযুক্ত কিনা এবং এ সংক্রান্তে জব্দতালিকায় উল্লেখ করা আছে কিনা?

৩। আবেদনে মামলার আলামত বিশ্লেষণপূর্বক সুনির্দিষ্ট তথ্য চেয়ে আবেদন করা হয়েছে কিনা বা মামলা প্রমানের জন্য কোন তথ্যাদি চাওয়া হয়েছে কিনা তা দেখা হয়।

৪। প্রদত্ত আলামত লকড থাকলে আনলকড করার জন্য কোন তথ্যাদি প্রদান করা হয়েছে কিনা তা দেখা হয়।

৫। জব্দ তালিকা সঠিকভাবে করা হয়েছে কিনা বা আলামতের পূর্ণাঙ্গ বর্ণনা জব্দতালিকায় উল্লেখ করা না হলে ঐ ফেরত প্রদান করা হয় বা সংশোধন করে পাঠানোর জন্য অনুরোধ করা হয়।

Forensic Tools & Software used for Analysis for Forensic Opinions

For Mobile Forensic

- Cellebrite
- Oxygen Detective
- MSAB
- CellXtract Device
- MD-RED/NEXT
- Salvation Data

For Internet Forensic

- IEF & Open Source Investigating Tools

For Computer Forensic

- Access Data FTK Forensic
- EnCase Forensic

- EnCase Endpoint Investigator
- Tableau Disk Duplicator
- Image Master SOLO
- Tableau Imager
- Magnet AXIOM
- BATVOX
- DVR Examiner

ডিজিটাল ফরেনসিক ল্যাবের প্রতিবন্ধকতা সমূহ

১। ডিজিটাল ফরেনিক ল্যাব প্রয়োজনের তুলনায় খুবই কম মাত্র তিনটি। অধিকাংশ মামলার আলামত তদন্তকারী কর্মকর্তারা সিআইডি, ডিজিটাল ফরেনসিক ল্যাবে পাঠিয়ে থাকেন। অন্য দুটি ল্যাবে মামলার আলামত পাঠানোর পরিমান তুলনামুলক কম।

২। প্রতিটি ডিজিটাল ফরেনসিক ল্যাবে প্রয়োজনীয় সংখ্যক ডিজিটাল ফরেনসিক বিশেষজ্ঞ নাই। যারা আছে তাদের অনেকেই বিষয়ভিত্তিক একাধিক প্রয়োজনীয় প্রশিক্ষন প্রাপ্ত নয়।

৩। ফরেনসিক টুলস ব্যয়বহুল হওয়ায় প্রতিটি ল্যাবে বিদ্যমান বিশেষজ্ঞ অনুপাতে ফরেনসিক টুলসের পরিমান অপ্রতুল।

৪। কোন সোস্যাল মিডিয়ার সাথে বাংলাদেশ সরকারের কোন ধরনের তথ্য আদান-প্রদানের চুক্তি এখন পর্যন্ত নাই, যা সাইবার ইনভেস্টিগেশনের পথে বড় অন্তরায়।

Thank
You